USER ACCESS MANAGEMENT

Date of adoption: 23 May 2017
Council resolves to adopt the under-mentioned revised policy as the Information Technology Policy of the DR BEYERS NAUDE LOCAL Municipality

Contents **Page**

1. INTRODUCTION

The purpose of this policy is to prevent unauthorized access into Dr. Beyers Naudé Local Municipality (BNLM) information systems. The policy describes the registration and de-registration process for all SBDM information systems and services

This policy applies to new employees, exiting employees and change in access requirements in terms of changes in employee’s positions or responsibilities.

2. USER ACCESS MANAGEMENT

2.1 New Users

Access to the municipality’s information services is controlled through a formal user registration initiated by a formal notification from Manager: Corporate Services.

Each user is allocated a unique User ID (username) for identification and accessing network resources (i.e. email). The use of group IDs is only permitted where they are suitable for the work carried out (i.e. Training).

Each user will be given a copy of the Employee Intake Form to provide written proof of their access rights provided, signed by the Systems Administrator after being inducted by Manager: Corporate Services.

The user signs the form indicating that they understand the conditions of access. Access to all municipality systems is provided by ICT Unit and can only be started after proper procedures are completed.

A new user will be set up upon receipt of the written notification but not made available, until the individual’s commencing date. ICT Unit will maintain a record of all requests in a folder named “New Users” in the ICT Unit.

2.2 Change of User Requirements

Changed requirements will normally relate to amendments to users’ access rights to applications as well as network access.

A request for additional access rights or removal thereof, must be made in writing (email or hard copy) by the employee’s Supervisor/Manager and must be directed to the Systems Administrator.

The request is free format, but must state:

- Name of person making request
- Job title of the employee
- Application or network access to be provided or removed
- Effective date of access rights provided or removed

Changes will be made on receipt of a properly completed request and the completed requests will be filed under “access change requests” in the ICT Unit.

2.3 Termination of Users

As soon as an individual’s contract with the municipality is terminated through either end of contract or resignation, all his/her access rights to the system must be revoked. As part of the employee termination process Manager: Corporate Services (or the Manager responsible for a Service Provider) will inform the Systems Administrator of all exiting employees and their date of exit.

All notifications will be kept in a file called “Terminated Users” in the ICT Unit. Additionally, Systems Administrator will positively confirm exiting employees with Manager: Corporate Services, each month. Unless otherwise advised, the Systems Administrator will delete network access for all exiting employees at 16:30 on their exit date**. (Old user ID’s are removed and not re-issued)**. This will include access to all network services. The Systems Administrator will inform Third Party application owners of exiting employees to ensure that the respective systems are updated accordingly.

All exiting employees are expected to hand over current files within their workgroup. User’s information will be left in its existing home directory; however, ICT Unit can move the employee’s files to specific areas if requested. It is the responsibility of the ICT Unit to make sure that all of the hardware and software is returned by the Employee and recorded in the Employee ICT Termination Form.

Responsibility of the Systems Administrator to do the following within 24 Hours of receiving the completed ICT Termination Form from HR:

- Disable or delete the Domain Account
- Disable or delete the Email
- Arrange Forwarding of Emails
- Remove/disable Program Access, Remote Access.
- Etc.

Once all of the above has been completed the ICT Unit must sign and file the ICT Termination Form.

3. PRIVILEGE MANAGEMENT

Administrative privileges are the highest level of permission that is granted to a computer user. In business and networked systems, this level of permission normally allows the user to install software, and change configuration settings. Only the System Managers or System Programmers are granted administrative privileges. The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached.

Privileged access must be authorized by the Director: Finance and Corporate Services, using the request form shown. All completed forms, both current and expired, will be held by the Systems administrator who is authorized by the completed form to set up the access specified.

All requests for access outside normal services must be supported by a completed and authorized Privilege Access form. The Senior Manager: Finance will maintain a master list of privileged accesses, which are in use, and this will be checked and confirmed by the Systems Administrator on a three-monthly basis. The list will identify all separate logons for each system and service.

4. USER PASSWORD MANAGEMENT

Password format and general rules are held within the ***Code of Conduct (8.3)***. Temporary access may be granted on a need to use basis. Such logons may be granted by the Systems Administrator and must be recorded on the normal form. Temporary logons must be identified by a specific login (starting TEMP****) and must be deleted immediately after use.

4.1 Change of User Password

Where a user has forgotten his/her password, the ICT Unit is authorized to issue a reset. Upon receipt of such a request the ICT Unit will:

- Ensure the request is logged.
- Confirm the identity of the user by question about existing services/access or by reference to a work colleague
- Issue a temporary, single use, password which will enforce the user to change the password at first logon.

4.2 Password Lockout

When an employee inputs an incorrect password 3 times, the employees access into his/her account will be locked.
The Reset Lockout Counter is set to a period of 24 hours. An employee may attempt to log into his/her account after the period of 24 hours has elapsed. Where an employee requires immediate access, the employee is required to contact the ICT Unit to unlock his/her account.

5. REVIEW OF USER ACCESS RIGHTS

The Systems Administrator will institute a review of all network access rights at least twice a year (January and July), which is designed to positively confirm all users. Any lapsed or unwanted logons, which are identified, will be disabled immediately and will be deleted unless positively reconfirmed.

At least twice a year the Systems Administrator will institute a review of access to applications. This will be done in cooperation with the application owner and will be designed to positively re-confirm all users. All other logons will be deleted.

The review will be conducted as follows.

- The Systems Administrator will generate a list of users, by application.
- The appropriate list will be sent to each Application owner who will be asked to confirm that all users identified are authorized to use the system.
- Any user not confirmed will have his/her access to the system removed.
- The Systems Administrator will maintain a record of -
- Lists sent over to Department Heads
- Department Heads responses
- A record of action taken by System Manager
- The review will be conducted in January and July
- The Senior Manager: Finance will then review the process accordingly.

The above processes will be followed for user access rights to the financial system (APPX) of the municipality

6. AUDIT LOGS

Audit log reports should be routinely generated and reviewed by the Systems Administrator for user accounts and evidence of the review should be retained for future reference.

Additionally, management should ensure that the job description of the IT Systems Administrator is reviewed and updated in order to align with current duties.

The following Audit Policy settings should be enabled:

- Audit Object Access
- Audit Privilege Use
- Audit Process Tracking

The Audit Logs on the Active Directory will be reviewed by the Systems Administrator and ICT Unit on a weekly basis.

7. REVIEW

This policy shall be reviewed at least annually.

8. Annexure A: Employee Intake Form

EMPLYOEE NUMBER:_

1.EMPLOYEE INFORMATION (To be completed by Manager: Corporate Services)			
First Name:		Start Date:	
Surname:		Residential Address:	
Work Ext No:			
Cell Phone No:			
Position:	_	Manager:	
Department:			
2.HARDWARE & SOFTWARE REQUIREMENTS (To be completed by Systems Administrator)			
Personal Computer:	Desktop	**USB Hard Drive:**	
	Notebook	Make:	
Make:		Model:	
Model:		Serial Number:	
Serial:		Asset Number:	
Asset Number:		**3G Dongle:**	
Warrantee Status:		Contract Number:	
Printer to be added:		Contract type:	
Primary Printer:		Contract cell number:	
Secondary Printer:		Serial Number:	

Color / Black only:		Asset Number:	
Telephone:		**Software version:**	
Extension Number:		Windows	
Serial Number:		Microsoft Office	
Asset number:		Antivirus	
Tablet:			
Make:			
Model:			
Serial:			
Asset Number:			
2.LOGON DETAILS (To be completed by Systems Administrator)			
Username:		**Access to Network Drives:**	
Password:		Departments:	
Network Domain:		User Files:	
Email Address:		Promun:	
Internet Access:		IMQS:	
Remote Access:		Corporate Services:	

Sections 2 & 3 have been authorized by the following departments:

ICT Unit:		**Director Corporate Services:**	
Name:		Name:	
Date:		Date:	
Signature:		Signature:	

The employee has read the User Access Management Policy and fully understands it. The employee has paid particular attention to the ICT Code of Conduct.

Furthermore, the employee takes full responsibility for the ICT Equipment that has been allocated to them.

Signing in Acceptance of All listed above:

Name:	
Signature: _	
Date:	

9. Annexure B: Employee ICT Termination Form

1.EMPLOYEE INFORMATION (To be completed by Manager: Corporate Services)			
First Name:		Start Date:	
Surname:		Residential Address:	
Work Ext No:			
Cell Phone No:			
Position:		Manager:	
Department:			

2.ICT ASSET RETURN (To be completed by ICT Unit)	
Asset	**Comment**
Desktop	
Laptop **with charger**	
Tablet **with charger**	
Telephone	
Modem (3G)	
3G Sim card	
Printer	
USB Flash Drive	
External Hard Drive	
Software Disks and License Keys	
Other:	
Other:	
Other:	
Other:	
Other:	

3. ICT UNIT CHECKLIST	
3G Cancelled	
Remove Appx System	
Email Disabled	
Domain Account Disabled	
Program Access Revoked (PROMUN, MUNADMIN)	
Remote Access Revoked	
All Municipal Data Backed Up	
Other:	
Other:	
Other:	
Other:	

All ICT Equipment Collected / Received □ Yes □ No

Remove All Company Related Data and Software □ Yes □ No

ICT UNIT

Systems Administrator / ICT Technician:

____

Signature: ______________________________

Date: ______________________________